

Assuring Physical Security of a Subscriber Line Device

Field of the Invention:

The present invention relates to equipment that can remotely access a network and
5 more particularly to the security of such equipment.

Background of the Invention:

Insuring that only authorized individuals or authorized equipment can connect to
network or to a server is very important. If a client is connected to a server or a
10 network by a POTS or ISDN line, caller ID, or a call-back mechanism can be used to
insure that a call is coming from a particular location. Telephone caller ID allows one
to insure that an incoming call is coming from a particular telephone line. A call back
technique can also be used to insure that a device connected by a POTS or ISDN
line is connected via a particular telephone line or location.

15 The packets transmitted by client devices which have a broadband connection do
not specify the physical location at which the packets originated. Security for
broadband connections is often accomplished by storing an encrypted "key" on a
client machine. Security in such a system is enforced by checking to insure that a
20 client requesting access has this key stored on the client. However, if a device with
a stored key is stolen is stolen, this key is also stolen. A stolen client machine with a
stored key, can be at a different location; however, when a server interrogates the
client, it will find the required key stored on the client.

25 The present invention is directed to insuring that a client device is in fact connected
to the network from a known location. That is, the present invention insures that a
client device is not seeking access to a network after it has been moved from a pre-
established location.

Summary of the Invention:

30 The present invention is directed to adding a layer of security to a network client
device that is connected to a network via a broadband connection. The security
provided by the present invention takes into account the physical location of the

client device . The security provided by the present invention insures that the client machine has not been moved from its authorized or pre-established location.

With the present invention, a check is made to insure that the machine connected by
5 a broadband connection is located at its assigned location. If this check finds that the client machine is not at its assigned location, the broadband network connection is inhibited or terminated.

One embodiment of the invention takes advantage of the fact that most clients
10 connected to a network via broadband, also have a POTS or ISDN connection to the outside world. With this embodiment of the invention, a client connected to a network with a high speed broadband connection, uses a caller ID mechanism or a callback mechanism on a slow speed POTS or ISDN connection to insure that the client is located at an assigned location.

15 In another embodiment of the invention, a GPS (global positioning system) mechanism is included in the client machine. When the client is connected to a network, a server can both check a encrypted key to insure that the client is an authorized client and the GPS data to insure that the client is at an assigned
20 location.

Description of the Drawings:

Figure 1 is a system diagram of a first embodiment of the invention with a client
25 machine connected to a network via a cable modem.

Figure 2 is a flow diagram illustrating the operation of the first embodiment of the invention.

30 Figure 3 is a block diagram of a second embodiment of the invention.

Figure 4 is a flow diagram illustrating the operation of the second embodiment of the invention.

Detailed Description of embodiments:

There are a variety of known broadband technologies that can be used to connect a client device to a network via a broadband connection. Two of the widely deployed technologies are "Cable" and "DSL". Security is an important consideration when a client connects to a network via a broadband connection. Frequently, security is implemented by storing an encrypted key on a client machine. When a client machine seeks to connect to a server, the server interrogates this key to insure that the client machine is authorized to access the server. Often a password (alone or a password together with an encrypted key) is also used to insure security.

However, a stored encrypted key or a password cannot be used to insure that a broadband connected client machine has not been moved from its assigned location. The present invention provides a layer of security that insures that a client machine is physically located at an assigned or pre-established location. The present invention can be used alone or in combination with other prior art security mechanisms.

The present invention can, for example, be used to verify that a client machine has not been stolen and moved to a new location. The present invention provides an alternative or additional mechanism for insuring network security for a client machine connected to a network with a broadband connection.

A first embodiment of the present invention is shown in Figure 1. The system shown in Figure 1 includes a client device 10 that is connected to a network server 16 via a broadband cable. The client 10 includes a cable modem 10C and an interface 10T to the normal telephone network 12. The client device 10 also includes an initialization program 10P. The client device 10 could for example be a personal computer or a network router. The telephone connection 10T could for example be a conventional modem or it could be some other type of conventional telephone network interface.

The cable modem 10 is connected to a CMTS (Cable Modem Termination System) which is part of the broadband gateway 14. The broadband gateway 14 is

connected network server 16 through the Internet 15. Connecting devices to a network by cable systems is conventional and not further described herein.

The system operates as shown in Figure 2. When the client device 1 powers up,
5 (that is when the client device 1 is initialized) the initialization program 10P causes the device 1 to place a call to itself via telephone network interface 10T. For example, if the telephone line from the central office 12 has the telephone number 345-1212, the telephone interface 10T places a call to 345-1212. The telephone line to central office 12 has the conventional call waiting and caller ID features.

10 As indicated by block 205, when the telephone interface 10T receives the incoming call, it checks the caller ID number in a conventional manner. If the number matches the pre-stored number (in this case 345-1212) the client 10 continues its normal initialization process. If the numbers do not match, this indicates that the client
15 device 10 has been moved and connected via a different telephone line and the process terminates. The reason for this is that the caller ID number is associated with a particular physical telephone line, and not with the device connected to that physical line. The device which actually initiates a call on a particular line does not affect the caller ID number of that physical line. Telephone devices for placing calls
20 and checking called ID numbers are conventional and thus telephone interface 10T is not further described herein.

It is noted that the stored telephone number (against which the called ID number is matched) can be stored in the program 10P in an encrypted manner so that it can
25 not be changed other than by an authorized user. Various known security devices can be used to protect this number from an unauthorized change.

In alternate embodiments where Call Waiting and Caller ID features are not available, the telephone interface 10T modem can call to a special number which connects to a
30 call back device (not shown in the drawings) which initiates a call back process. In such an embodiment, initialization only proceeds if the device in fact receives the appropriate call back.

Naturally it should be understood that initialization program 10P also performs the other normal initialization operations.

The network server 16, can also authenticate the client using other conventional authentication processes. For example, a key stored on the client can be interrogated in a conventional manner to insure that the correct machine is trying to access the server.

In summary the first embodiment shown in Figure 1 adds a security mechanism that insures that a client machine has not been moved from its assigned location. This additional security measure can be used alone or together with other known security measures.

A second embodiment of the invention is shown in Figure 3. In this second embodiment of the invention, the client device 20 includes a cable modem 20C and an initialization program 20P similar to the first embodiment of the invention. Also similar to the first embodiment, the client 20 is connected to the Internet 25 and from there to a server 26. However, in this second embodiment of the invention, the client device 20 includes a "Global Positioning System" (GPS) unit 20G. The GPS unit 20G is a conventional receiver, that determines its actual physical position from satellite signals. The unit 20G determines its global coordinates (longitude and latitude) and stores them in a register (not explicitly shown in the drawings). Such a GPS unit is conventional and not further described herein.

When the client unit 20 is initialized, the initiation program 20P reads the coordinates determined by unit 20G. These coordinates are compared to coordinates previously stored in the client. If the coordinates match, it indicates that the unit has not been moved, and the initialization proceeds. If the coordinates do not match, the initialization is terminated. It is noted that the coordinates can be stored in the program 20P in an encrypted manner so that they cannot be changed other than by an authorized user.

The operation of the system is illustrated in Figure 4 which illustrates the relevant steps performed by initiation program 20P in conjunction with GPS unit 20G.

Naturally it should be understood that initialization program 20P also performs the other normal initialization operations.

5 The operations occur when the unit powers up as indicated by block 302. The GPS unit 20G determines its coordinates as indicated by block 304. As indicated by block 305, a check is made to determine if the coordinates determined by GPS unit 20G match those stored in initialization program 20P. If the numbers match the initialization proceeds in a normal manner as indicated by block 307. If the coordinates do not match the initialization process stops.

10 In still another alternate embodiment, when the numbers do not match, a signal is sent to a securityh server by cable via cable modem 20C and CMTS gateway 24. The signal sent to the security server can include the coordinates indicated by GPS unit 20U, thereby giving an indication of the location of a possibly stolen unit.

15 Various other embodiments of the invention are also possible. There are a variety of alternative techniques that can be used to connect a remote client to a server via the internet. Embodiments utilizing various broadband network technologies are possible.

20 For example another embodiment utilizes the Digital Subscriber Line (DSL) technology and protocol. DSL allows high speed data communication over copper telephone lines between end-users and central offices. DSL allows one pair of wires to be used for a regular telephone connection (using low frequencies) and a
25 broadband digital connection (using higher frequencies). This type of connection is becoming popular in the United States and it is even more popular in Europe.

30 An embodiment using DSL could be similar to the embodiment shown in Figure 1, except that instead of a cable modem and a CMTS gateway, such an embodiment would include a single pair of wires connecting the client machine to the gateway device. These wires would carry both a normal POTS connection and a broadband connection. The operation of such an embodiment would be similar to the first embodiment except that the broadband and the POTS connection would be via a single pair of wires.

It is noted that the various embodiments of the invention could be used singularly or in combination for added security. For example, in still another embodiment, both the embodiments shown in Figures 1 and 3 could be implemented in the same client.

5 Such an embodiment would both call itself and check the caller ID and compare GPS coordinates before initializing.

Likewise the location checking mechanism described herein could be used alone or in combination with other security mechanisms such as the used of an encrypted
10 stored key and password. Such an embodiment would both check a caller ID as does the first embodiment or check GPS coordinates as does the second embodiment and interrogate a stored encrypted key and/or a password. The number of security techniques used in any particular instance is a matter of engineering choice depending on the circumstances.

15 In the above described embodiments, the check of the physical location of the client device is performed at the time the device is initialized, in other embodiments, this check could be performed at various other time. For example, the physical location check could be performed each hour of operation or each day of operation, etc.

20 In the above described embodiments, the initialization process is terminated if the actual physical location of the device does not match some pre-established physical location. It is noted that instead of terminating the initiation process, various the client device could be prohibited from connecting to the network by various other
25 means such as by disabling the cable modem or other broadband connection.

It is noted that herein the terms client machine and client device are used interchangeably to mean the same thing. Namely, as used herein both the terms "client device" and "client machine" refer to a client connected to a network by a
30 broadband connection. The network 15 and 25 can be a Local Area Network (LAN) or a Wide Area Network (WAN). Networks 15 and 25 could for example be the Internet.

While various embodiments of the invention have been shown, it will be understood by those skilled in the art, that various other changes in form and detail may be made without departing from the spirit and scope of the invention.
The scope of the invention is limited only by the appended claims.

5

I claim: